suez

SUEZ Water Delaware
2000 First State Boulevard
Wilmington, DE 19804
TEL 302-252-3035
FAX 302-633-5910
www.mysuezwater.com

ANNUAL CYBERSECURITY QUESTIONS

PSC Docket No. 16-0659

Planning/Risk Management

Is your cybersecurity plan regularly reviewed and audited?...................................... Yes
Internally or externally?.. Both

Has your plan been reviewed recently? .... Yes
If not how often is it reviewed?...Annually

Do you assess vulnerabilities to your system and assets? .... Yes

Do you assess threats to your system and assets? .... Yes

Do you prioritize risks?... Yes
And what processes do you use? ....

The following process are implemented in our IT Risk & Security Program:

- Monthly External Vulnerability Scans are performed.
- On demand Internal Vulnerability Scans are performed.
- Pre-implementation Security/Risk Assessments for approved Projects.
- Quarterly PCI Security Scans for any websites which process credit card data.
- Documenting process outcomes in the IT Risk and Security Register.
- Monthly security metrics are provided in a report to management.
- An IT-GRC (governance risk & compliance) tool is used to map all NIST controls to our policy framework.
- A risk register is maintained to capture and track significant risks.

Personnel and Policies

Are background checks being conducted upon hire? .... Yes

Do you provide internal cyber security training for all employees? .... Yes

- Suez N.A. regularly trains employees with a variety of "Security Awareness" training campaigns.

Do you provide enhanced internal cyber security training for those that are actually in the utilities operating network?.. Yes

Are there structural and/or organizational policies and procedures in place that allows the utility to able to address or think through these things (cybersecurity issues)?..... Yes

Are there managerial and operational controls in place? .... Yes

How quickly is access to those personnel who quit/fired eliminated? .... At time of termination

Do you have certain employees that are assigned as cybersecurity personnel? .... Yes
Or outsourced? .... N/A

- Suez N.A. has a dedicated IT Risk & Security team in place.

Do you have specific practices and policies in place about how your private customer data should be handled? .... Yes
Contingency plans for breach of data? .... Yes

Are recovery activities communicated to internal stakeholders and executive and management teams? .... Yes

Do you screen vendors and third parties that have access to cyber control systems? Yes

Standards and Guidelines for Reporting

Do you have a disaster recovery plan? (The plan itself should not be made public.). Yes

Do you have separate plans for separate business units in the company? .... Yes

Are you reporting to the necessary agencies in regards to your plan? .... Yes

Are response and recovery plans regularly tested? .... As required

Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed? .... Yes

- Subscribed to Water ISAC Security & Resilience Updates.

Do you have a list of contacts for cybersecurity information sharing? (i.e., Federal and state emergency management, law enforcement, National Security, and Any others?)
.... Yes

Should the Commission create guidelines or regulations to ensure utilities are properly managing cyber security issues? ....

- SUEZ provides a high level of cyber security coverage, both for systems and customer data, and will strive to comply with any guidelines or regulations set down by the regulators for the locations in which we operate.